

REPLACEMENT SHEET ROTATION ROTATION (m) 23 S LEFT ROTATION 8 (-) 222222 5 ZS1 PC2 PERMUTED PERMUTED 22 FIG. 1B \$ ₩ 32 XOR PERMUTATIO 32 IP IN. INTAL

APPRICABLE J. L. CALVIUNAL et al.

ATOMEY DOKER NO. PL/3/2
Title: SNOLE-CYCLE HARDWARE IMPLEMENTATION OF CRYPTO
FUNCTION FOR HIGH THROUGHPUT CRYPTO-PROESSING
RESPONSIVE to Official Communication dated: February 21,2008

REPLACEMENT SHEET ROUND 1 ROUND ROTATION LEFT ROTATION 28 28 1 PC1 PERMUTED CHOICE S S Ψ ROTATION ROTATION 28 28 ISI EFI ङ PC2 PERMUTED CHOICE } PC2 PERMUTED FIG. 2A 岙′ P PERMUTATION 쭚 EXPANSION XOR DATA 32 32 IP INITIAL PERMUTATION (m Š INIT VAL/ACCUM

Applicant: J. L. CALVIGNAC et al. Attorney Docket No. P27325
Title: SINGLE-CYCLE HARDWARE IMPLEMENTATION OF CRYPTO
FUNCTION FOR HIGH THROUGHPUT CRYPTO-PROESSING

